AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Alexander Harrison Vance, Special Agent with the Federal Bureau of Investigation (FBI), Kansas City, Missouri, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent for the FBI since January 2020. As part of my duties as a Special Agent, I am assigned to investigate violations of federal law, specifically the online exploitation of children. This includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the detection and investigation of criminal offenses. I have written, executed, and/or participated in the execution of numerous search warrants. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained expertise in these investigations through training, discussions with other law enforcement officers, and everyday work related to conducting these types of investigations.

2. At all times throughout this affidavit I use the terms "Child Sexual Abuse Material (CSAM)" and "child pornography" merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor," and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2256 (See Definition Section below).

3. This affidavit is made in support of an application for a warrant to search the place described in **Attachment A-1** – the premises located at **105 SE 350th Road, Warrensburg, Missouri 64093** (hereinafter identified as the "SUBJECT PREMISES"), as well as the person described in **Attachment A-2 – Naythan Justin Henopp** (hereinafter referenced as **Naythan HENOPP** or **HENOPP**) – for the items described in **Attachment B**. As will be shown below,

there is probable cause to believe **HENOPP**, currently residing at the SUBJECT PREMISES, has possessed and transmitted child pornography, in violation of Title 18, United States Code, Section 2252.

4. This affidavit is based upon information I have gained from my investigation, my review of other investigative reports in this case, conversations with other investigators working on this case, as well as my training and experience. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2251 and 2252, are presently located at the SUBJECT PREMISES and on **HENNOPP's** person.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. §§ 2251(a) and (e) (production of visual depictions of minors engaging in sexually explicit conduct), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution and/or receipt of a visual depiction of a minor engaged in sexually explicit conduct) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct).

a. 18 U.S.C. §§ 2251(a) and (e) prohibit a person from knowingly using, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, or attempting to do so;

b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual

depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

TECHNICAL INFORMATION REGARDING KIK

6. Kik is an online service, owned and maintained by Medialab Inc. Kik is a free application available on numerous platforms, including, but not limited to, Apple devices, Android devices, tablets, and cell phones. A Kik user registers for an account with a user provided email address, and is able to send and receive messages, live images and/or videos on any mobile device with a Wi-Fi, or cellular connection. A Kik user is assigned a username, which is constant for the

duration of their account, but can use various "vanity names" for their account. Kik c/o Medialab Inc. maintains records for its users, including but not limited to, account creation IP addresses, IP address logs, account creation email addresses, and device IDs.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

7. On Wednesday December 7, 2022, an FBI Task Force Officer was acting in an undercover (UC) capacity as part of the Metropolitan Police Department-Federal Bureau of Investigation ("MPD-FBI") Child Exploitation Task Force, operating out of a satellite office in Washington, D.C. In that capacity, the UC entered a private KIK group in which the UC serves as one of the group's administrators. This group is known to the UC as a place where people meet, discuss and trade original images and videos of underage children.

8. On Wednesday December 7, 2022, at approximately10:09AM EST, a KIK user using the screen name, "longfellowdon187" entered the group and stated, "35 male Missouri and [redacted]" At approximately 12:31 AM UTC, another member of the KIK group posted a video of a minor [redacted] sleeping. An adult hand is seen in the video reaching over to the minor [redacted] and moving the minor [redacted] underwear so as to expose the minor [redacted]. The UC asked "longfellowdon187", subsequently identified as **HENOPP** to private message him within the KIK application.

9. During the course of the private chat with the UC **HENOPP** verified that he has a [redacted]. **HENOPP** initially sent a live camera picture of himself then sent a preexisting picture of himself with a [redacted] minor [redacted] who he identified [redacted]. In the preexisting picture both **HENOPP** and [redacted] fully clothed. The picture captures the faces of both **HENOPP** and [redacted] During the

chat, **HENOPP** stated [redacted] and later sent an image of a minor [redacted] in the shower completely nude, [redacted] Additionally, during the chat, **HENOPP** stated that [redacted] and he wanted to try to put [redacted] "dead asleep and play."

10. On December 8, at approximately 1:34am **HENOPP** sent 3 images to the group. The first image depicts a child laying in a bed wearing purple pants. [redacted] is lying on [redacted] stomach on top of blue bedding and [redacted] face is covered with a grey blanket. The second image depicts the same child and focuses on the child's bare feet. An adult male is behind [redacted] holding his erect penis. The third photo depicts the same child. In this photo the child appears to be sleeping and [redacted] face is exposed. Two pillows are located near the head of the child, one is purple in color and the other is pink in color. An adult is standing behind the child's head with his erect penis exposed. [redacted] A male is standing behind the child's head with his erect penis exposed.

11. **HENOPP** commented to the group as he was posting these images that the minor [redacted] pants were too tight to pull down. Another KIK user tried to encourage him to take [redacted] pants off slowly, **HENOPP** responded, "Yea try again when [redacted] wears [redacted] shorts to bed."

12. On December 8, 2022, at approximately 9:20 AM **HENOPP** continued communications with the UC. The messages included the following:

- UC: Can't wait to see [redacted] though, where did you end up cumming?
- UC: U have any other pics that u didn't already send to the group

At approximately 1:14 PM, **HENOPP** and the UC discussed the following:

- **HENOPP**: [redacted] ass
- **HENOPP**: Layed up next to [redacted] and jerked off on [redacted] butt

- **HENOPP**: Any pics of [redacted]
- UC: Let me look
- UC: U have any more from last night
- **HENOPP**: No tonight trying more gonna drug [redacted]

13. On December 8, 2022, during a review of the images provided by **HENOPP** via KIK, as referenced in paragraph 10 above, investigators observed what appeared to be a tattoo on the right hand of the adult male whose penis is located near the head [redacted]. A review of a Ruth HENOPP's Facebook page shows an image of **HENOPP**. In the image a tattoo is clearly visible on his right hand.

13. On December 8, 2022, an emergency disclosure form was submitted to Kik c/o MediaLab Inc. requesting subscriber information and IP logs associated with username longfellowdon187. On the same day, Kik responded to the request providing a display name of "Don Longfellow", an unconfirmed email address of eightlygsyndicate@gmail.com, a device description of iPhone, and IP logs spanning 11/10/2022 through 12/08/2022. Examination of the IP logs yielded a combination of AT&T Wireless and Charter Communications IP addresses.

14. An emergency disclosure request was submitted to Charter Communications for subscriber identification and service address information associated with IP address 172.221.220.200. Charter responded to the request identifying the subscriber as Dustin Johnsen, at service address 105 SE 350th Road, Warrensburg MO 64093.

15. Upon receipt of this information, FBI personnel used available open source, commercial, and law enforcement sensitive databases to fully identify the suspected user of Kik account longfellowdon187 as **Naythan Justin HENOPP** (DOB: [redacted] SSN: [redacted] FBI: [redacted]; AT&T telephone number: [redacted]). **HENOPP's** wife was

identified as Ruth Katherine Henopp (DOB: [redacted]). Social media accounts belonging to "Naythan" (www.facebook.com/[redacted]) and "Ruth" (www.facebook.com[redacted]) were also identified. Review of publicly viewable photographs on these profiles yielded numerous images depicting individuals visually matching **HENOPP** [redacted].

16. On December 8, 2022, Affiant observed the previously referenced images sent by Kik user "longfellowdon187." The Affiant compared the shared images with social media photographs, which were observed on **HENOPP's** personal Facebook page. A minor [redacted], appeared to be the same minor [redacted] as seen in the images sent by Kik user "longfellowdon187."

DEFINITIONS

17. The following definitions apply to this Affidavit and **Attachment B** to this Affidavit:

a. "Child Erotica," as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons, and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e)

lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

d. "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

e. "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards

(MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

18. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

19. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

20. With the advent of digital cameras and cell phones, images can now be transferred directly from a smart phone onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

21. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

22. A smartphone, or smart phone, is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Early smartphones typically combined the features of a mobile phone with those of another popular consumer device, such as a personal digital assistant (PDA), a media player, a digital camera, or a GPS navigation unit. Modern smartphones include all those features plus the features of a touchscreen computer, including web browsing, Wi-Fi capability, and apps. Frequently, smartphones also include removable storage devices, or SD cards, where users can store data, including picture and video files.

23. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, and store and view movie and picture files.

24. The Internet and its World Wide Web afford collectors of child pornography several different venues and social media platforms for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

25. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as cloud storage, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Even when users delete data, remnants or evidence of that data may still remain within the computer data.

27. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

SEARCH METHODOLOGY TO BE EMPLOYED

28. The search procedure of electronic data contained in computer hardware, computer software, memory storage devices, and/or cell phones may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, memory storage devices, and/or cell phone to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to

determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

SPECIFICS OF SEARCH AND SEIZURE OF CELLULAR PHONES

29. Searches and seizures of evidence from cellular phones commonly require agents to download or copy information from the cellular phone to be processed later in a laboratory or other controlled environment. This is almost always true because of the following:

a. Cellular phones can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching cellular phones for criminal evidence can be a technical process requiring forensic tools and a properly controlled environment. The vast array of hardware, software, and applications available makes it difficult to know before a search which tool will be necessary to analyze the system and its data. The search of a cellular phone is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE PRODUCTION, DISTRIBUTION, OR POSSESSION OF CHILD PORNOGRAPHY OR IN THE CONSPIRACIES OR ATTEMPTS TO COMMIT THOSE CRIMES

30. As set forth above, probable cause exists to believe **HENOPP** attempted to produce, receive, and possessed child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who produce, receive or possess child pornography, or who conspire or attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, receive or possess child pornography, or who attempt or conspire to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, receive or possess child pornography, or who attempt or conspire to commit these crimes often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondences, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who produce, receive or possess child pornography, or who attempt or conspire to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly. These collections maybe in separate locations near the residence, such as outbuildings, so as to avoid detection by other residents.

e. Those who produce, receive or possess child pornography, or who attempt or conspire to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individual with whom they have been in contact and who share the same interests in child pornography.

f. Those who produce, receive, or possess child pornography, or who attempt or conspire to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Those who use cell phones to commit such offenses often use multiple phones to commit these offenses and/or discard old devices used to commit the offenses in favor of new ones, and continue offending utilizing the new device.

31. Based on my training and experience as a law enforcement officer, as well as my experience personally using and owning cell phones, I know that individuals who use cell phones most often keep them on their persons and in their residences.

CONCLUSION

32. Based on the foregoing, I submit there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in **Attachment B** of this Affidavit, are located at SUBJECT PREMISES, described in **Attachment A-1** or on the person of **Naythan Justin HENOPP**, described in **Attachment A-2**. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES and for the person of **Naythan Justin HENOPP** described in **Attachments A-1 and A-2**, authorizing the seizure and search of the items described in **Attachment B**.

33. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in **Attachment B.**

Alexander Harrison Vance
Special Agent
Federal Bureau of Investigation

Telephonically
Sworn and subscribed before me
This 8th day of December 2022

Honorable Jill A. Morris
UNITED STATES MAGISTRATE JUDGE